

Information security at Atea

Contents

Introduction

Atea is committed to maintaining robust information and IT security practices to safeguard both internal assets and customer information. To achieve this, we have implemented a comprehensive Global Information Security Management System (ISMS) based on ISO 27001 standards. Our ISMS is further reinforced by GDPR-specific controls and essential IT security measures.

Within Atea, our security organization diligently oversees and manages information and IT security in alignment with the ISMS and relevant legal requirements. We have appointed a Group Chief Information Security Officer (CISO) to lead security initiatives across the Group, along with local Information Security Officers (ISOs) within each Business Unit. Additionally, Atea has Data Protection Officers (DPOs) in all Atea countries. For contact information regarding ISOs, please visit Atea.com/information-security/.

Information security policy

Atea maintains an Information Security Policy that outlines our strategic objectives, ambitions, and goals related to information security. This policy is globally applicable and undergoes annual updates.

Information Security Management System (ISMS)

Atea's ISMS outlines thorough protective measures for safeguarding information and assets. These measures span administrative, technical, and behavioral domains. Additionally, the ISMS defines roles and responsibilities necessary for maintaining security. It encompasses security policies, underlying requirements, processes, and guidelines.

- ATEAIS-P001 Information Security Policy
- ATEAIS-P002 Access Control Policy
- ATEAIS-P003 Asset Management Policy
- ATEAIS-P004 Cryptography and Key Management Policy
- ATEAIS-P005 HR Security Policy
- ATEAIS-P006 Information Security Compliance Policy
- ATEAIS-P007 Information Security Continuity Policy
- ATEAIS-P008 Information Security Incident Management Policy
- ATEAIS-P009 Network Security Policy
- ATEAIS-P010 Operations Security Policy
- ATEAIS-P011 Organization of Information Security Policy
- ATEAIS-P012 Physical and Environmental Security Policy
- ATEAIS-P013 Secure Development Policy
- ATEAIS-P014 Supplier Relationship Policy
- ATEAIS-P015 Acceptable Use of AI (coming 2024)
- Atea Information Security Risk Management Policy for Employees

Security Risk management

Atea diligently addresses security risk management across the entire organization. Recognizing its significance in information and IT security, we adhere to ISO 27001 requirements. Our risk management process aligns with the ISO 31000 standard for risk management and the ISO 27001 standard for information security.

Regular risk analyses are conducted, considering threats, countermeasures, and ongoing monitoring of dynamic conditions.

Handling of personal information

Atea places significant emphasis on the handling of personal data. We take all necessary precautions to safeguard privacy. This commitment extends to all personal data processing activities conducted by Atea.

Our ongoing efforts include strict adherence to the General Data Protection Regulation (GDPR). The GDPR framework encompasses policies, underlying requirements, processes, and guidelines, ensuring compliance and robust data protection practices.

- GDPR-P001 Data Protection Policy
- Data privacy policy (Country specific on local external websites).

Vital ITIL processes from a security perspective

Atea utilizes ITIL practices as a framework for its IT activities.

Atea's incident management process effectively handles incidents within its IT environments and managed services provided to customers. Security incident handling follows a Security Incident Response Plan (SIRP), and a dedicated Security Incident Response Team (SIRT) manages complex security incidents. Root cause analysis aligns with the problem management process.

All changes to Atea's environments follow the change management process, ensuring controlled and well-documented modifications to minimize risks and maintain stability.

Atea remains committed to robust data protection practices and compliance with industry standards.

Threat surveillance

Atea is continuously keeping updated on and acts on security threats and vulnerabilities. This is accomplished by Atea Group Security Advisory Board and Atea Group Cyber Security Board with cooperation by more than 200 Atea security consultants.

Our IT environments are periodically security tested and critical services exposed on the Internet are penetration tested annually by external party. These services are also vulnerability scanned internally every month.

We continuously measure and act on our Digital footprint posture following Security Scorecard rating with goal to stand on a higher rating than the industry standard.

Education and awareness

Atea prioritizes information security by continuously raising awareness among all employees. This includes ongoing education about actual threats and risks. New employees receive security training during their onboarding process. Additionally, Atea conducts internal phishing campaigns to enhance awareness, recognizing that Email Phishing remains a significant security concern.

Access Management

Atea adheres to the principle of least privilege access in accordance with ISO 27001. We enforce multi-factor authentication for all user access, complemented by conditional access rules. Additionally, Atea utilizes LDAP and SAML protocols to verify access between services and external SaaS platforms.

Physical Office security

Atea offices are protected according to ISO 27001. Offices with IT deliverables are certified according to ISO 27001.

Data Facility security

All Atea's utilized data facilities are ISO 27001 certified.

Business Continuity Management

Business continuity management serves as a safeguard, a form of insurance. It provides Atea and our clients with the assurance that even in the face of disaster, the impact will be mitigated. Atea maintains crisis management teams at both global and local levels to ensure uninterrupted business operations during critical events. Additionally, disaster recovery plans are in place for all essential services delivered by Atea.

Governance and reporting

Atea's information security framework is overseen by the Group Security department, which encompasses information security, data privacy, IT security, physical security, awareness, and compliance with laws and regulations. Led by the Group CISO, this team ensures robust risk management practices. Our managed services have a dedicated security team responsible for safeguarding our customers.

Strategic decisions related to security strategy are made by the Information Security Executive Council, led by the Group COO.

To address any deviations from our security framework, the Group Security Advisory Board investigates and proposes alternative solutions.

Privacy matters fall under the scope of the Privacy Advisory Board, led by the Group Privacy Officer.

Local Information Security Officers (ISOs) and Data Protection Officers (DPOs) report security status to the Group CISO. Additionally, Group CISO provides quarterly security updates to the Information Security Executive Council, while local ISOs report to their respective management teams.

IT Security measures

From a user perspective

Atea employees utilize devices configured with industry best practices. Our IT shields include antimalware with XDR protection, local firewalls, and IPS protection. DNS protection is enforced for web traffic, and all Atea devices have enforced disk encryption. Conditional access controls grant information access. We monitor patch status using Snow Risk Monitor and employ VPN solutions with conditional access rules for external network access. Additionally, we enforce information classification based on Atea's requirements and provide a password manager tool for secure password handling on all devices.

From an IT Infrastructure perspective

Atea safeguards our internal network with DDoS protection on Internet connections. Next-generation firewalls with IPS protection are deployed, and network segmentation minimizes lateral risk. Our servers adhere to best practices, featuring antimalware with XDR protection and local IPS protection.

Security Audit

All Atea Managed Services operations and environments are annually audited to fulfil ISO 27001 certification by external accredited ISO 27001 auditors.

- Atea Sweden Managed Services - ISO 27001 certified
- Atea Norway Managed Services – ISO 27001 certified
- Atea Denmark Managed Services – ISO 27001 certified, ISAE 3402 audited
- Atea Finland Managed Services – ISO 27001 certified
- Atea Baltics – Partly ISO 27001 certified
- Baltneta – ISO 27001 certified
- Atea Global Services – ISO 27001 certified
- Atea Logistics – ISO 27001 certified
- Atea Digital Services – ISO 27001 certified

Atea annually conducts an internal GDPR and Information Security Audit on all Business Units.

Management of vendors and subcontractors

Atea follows a back-to-back agreement practice with vendors and subcontractors. This ensures that they adhere to the same security requirements as Atea. New vendors and subcontractors undergo security controls to validate compliance with Atea's security standards. Additionally, Atea periodically assesses subcontractors for GDPR compliance, including information security controls.

ISMS document distribution

Atea Information Security Management System (ISMS) and other Atea documents referenced herein are distributed only following a formal request and a written non-disclosure agreement.